POSITION PAPER

BUSINESSEUROPE

17 October 2012

COMMISSION PROPOSAL ON A GENERAL DATA PROTECTION REGULATION

KEY MESSAGES

1 The General Data Protection Regulation should contribute to the achievement of greater harmonisation towards the establishment of a true Digital Single Market.

2 However, the Commission proposal is overly prescriptive and detailed in a way that creates more administrative burden and compliance costs for companies without a proportionate privacy benefit. In this way, it discourages digital innovation and competitiveness.

3 The proposal introduces far-reaching documentation obligations, data protection impact assessments, prior consultations and authorisations that will disproportionately increase administrative burden for companies with no benefits for consumers.

WHAT DOES BUSINESSEUROPE AIM FOR?

- BUSINESSEUROPE does not support the changes in the definition of data subject's consent compared to the current directive, as they will make the process too cumbersome and prescriptive. In case of continued business relationships, these requirements are an unnecessary supplementary administrative burden.

- The numerous provisions on secondary rulemaking (delegated and implementing acts) undermine legal predictability and risk neutralising the effectiveness of the provisions by complicating the data protection regime.

- Despite the fact that effective and high- quality enforcement is essential, the proposed sanctions are excessive and disproportionate. In our view, particularly in cases of first and non-intentional non-compliance, a warning procedure as well as pre-requisites for renouncing from inflicting sanctions should be considered.

- In addition, we are worried about the impact of the proposal on data processing in the employer/employee relationship. In several Member States, collective agreements and employees' consent to the processing of their data by employers

are also the basis of legal data processing. This practice should be maintained. Otherwise, administrative burden will increase while employees' situation will not improve.

- It is extremely important to clarify the distinction between the liabilities of the data controller and those of the data processor. Indeed, some confusion can be observed in several provisions of the regulation on this matter. Data processor obligations should continue to be controlled by and specified in contractual clauses between controller and processor.

BUSINESSEUROPE a.i.s.b.l
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

BUSINESSEUROPE

POSITION PAPER

17 October 2012

BUSINESSEUROPE COMMENTS ON THE COMMISSION PROPOSAL FOR A GENERAL DATA PROTECTION REGULATION

I. INTRODUCTION

The Commission adopted on 25 January 2012 proposals to review the current EU data protection framework (directive 95/46/EC). BUSINESSEUROPE will focus its comments on the proposal for a General Data Protection Regulation [COM(2012), 11].

We support the aim of the proposal to achieve greater harmonisation towards a Digital Single Market for Europe. In a data-driven age, it is important to get data protection rules right for European businesses and consumers and ensure legal certainty. Effective digital solutions, more competition across Europe and a more efficient public sector depend on citizen's trust in information and communications technology (ICT).

We also welcome the single Data Protection Authority (DPA) concept based on the "main establishment" of a company principle sometimes referred to as a "one-stop-shop" for compliance. This should simplify and streamline companies' relations with data protection authorities.

We are concerned about the overall approach to draft the proposal with respect to a data controller and not the enterprise as a whole. This could give rise to confusion as to what the main establishment is or where the "one-stop-shop" for compliance might be as an organisation could be a data controller in multiple Member States.

Furthermore, the proposal not only determines what obligations apply but how they are implemented in an overly detailed way without reflecting the realities of today's technologies and taking account of other specific regulation (e.g. consumer law, contractual law, employment law, collective agreements, national legislation on privacy, sectorial requirements). This will create unnecessary burden, increase costs without a proportionate privacy benefit, discourage digital innovation and competitiveness, as companies will be pushed to invest in administrative compliance rather than growth.

We believe that regulators need to craft the "what" is expected and remain clear and comprehensive regarding the "how". Accordingly, the proposal should provide enough flexibility to allow different organisations to implement the most effective technical and organisational measures, fit for the nature and structure of each respective organisation to ensure optimal data protection. Instead of the detailed and prescriptive rules an organisational accountability obligation would be more effective.

The proposal should have been more "future-proofed" by giving sufficient consideration to businesses' activity online and how it may change in a short amount of time. This is particularly relevant for work in the cloud. The requirement to inform individuals of the level of protection in any country to which their data may be transferred (Article 14(1g)) is not workable in practice in the context of data stored in the cloud. Article 30 also demands appropriate security measures to be agreed between processors and controllers, and here a form of security certification could be introduced for cloud

BUSINESSEUROPE a.i.s.b.l
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

service providers. In other areas, the proposal does not provide sufficient clarity as to who is responsible for data published via social media networks.

In addition, we are worried about the impact of the proposal on data processing in the employer/employee relationship. In several Member States, collective agreements and employees' consent to the processing of their data by employers are also the basis of legal data processing. This practice should be maintained. Otherwise, administrative burden will increase while employees' situation will not improve. In that respect, we also refer to provisions in articles 153-155 in the Treaty on the Functioning of the European Union (TFEU).

BUSINESSEUROPE will develop its concerns in its detailed comments below. If these shortcomings are not effectively addressed by Member States and the European Parliament, they will outweigh the positive elements of the Commission proposal.

II. DETAILED COMMENTS

DEFINITIONS

1. DEFINITION OF PERSONAL DATA

We believe that various key definitions in the Commission proposal suffer from ambiguities. This will adversely affect the aim of ensuring legal certainty and also impact other principles of the proposal such as consent and profiling.

Such an example is the linking of the definitions of "data subject" and "personal data", meaning that personal data is defined as "any information relating to a data subject". A person is a data subject as soon as he or she is reasonably to be expected traceable by "means reasonably likely to be used by the controller or by any other natural or legal person". In our view, this is too broad and lacks clarity. Moreover, naming for e.g. IP addresses and cookies as measures by use of which data subjects can be identified seems to broaden this definition of data subject. Combined with the recital 24 of the proposal which stipulates that such factors need not necessarily be considered as personal data in all circumstances, this blurs the legal framework. Therefore, a clarification is needed whether IP addresses, IP ports or cookies etc. are included in the definition "personal data" and if the answer is positive, what the circumstances referred to in recital 24 mean, when they shall not be considered as "personal data".

To offset possible huge cost of compliance and legal uncertainty a clear definition is needed making data "personal data" only when this is in the context of processing of this data where it is supposed to be "personal data".

One should consider the unintended consequences that an overly broad definition could have, especially when read in combination with the more explicit requirements of consent. The need to use IP addresses for a variety of security and authentication purposes both directly and indirectly would be undermined as bad-faith actors are unlikely to consent to the capture of such information if they believe it will be used to prevent the acts they are executing. This is an example of the need to tailor more

narrowly the draft in order to address specific and compelling public policy issues while not resulting in undue burden or unintended consequences.

2. DEFINITION OF LEGAL PERSONS

Furthermore, the proposal explicitly states (recital 12) that the protection afforded by the regulation should not be claimed with regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

From this wording, the reference to the undertakings seems to be only limited to those "established as legal persons" and not to undertakings in general. By contrast, the relevant element to identify an undertaking should be the economic activity (as stated in article 4, n. 15 "'enterprise means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity"). Therefore, it would be better to modify recital 12 in order to avoid misunderstandings, and to simply refer to "undertakings" in general, instead of "undertakings established as legal persons".

3. DEFINITION OF DATA CONCERNING HEALTH

In addition, the proposal defines data concerning health as information which relates to the physical or mental health of an individual, or the provision of health services to the individual. This definition is impossible to implement in practice.

Purely administrative data should therefore be excluded explicitly from this definition.

CONSENT (ARTICLES 4, 7 AND 8 AND LABOUR MARKET)

1. DEFINITION OF CONSENT

Individuals should have the right to make an informed choice about how their data will be processed. BUSINESSEUROPE believes that the provisions of the proposal on consent should not hinder a sensible and flexible processing of data and use of services.

We do not support the changes in the definition of consent as they will make the process too cumbersome and prescriptive. In case of continued business relationships, these requirements are an unnecessary supplementary administrative burden.

This is likely to turn consent into a box-ticking exercise rather than a way for data subjects to control their data. The number of forms and tick boxes that users need to complete will increase. Online services will be negatively affected, as users will be an additional click away from accessing the product, services, content they are interested in. It must remain possible for consumers to provide implicit consent i.e. in the process of registration.

In addition, online service providers would be seriously hindered, while the personal data they ask for (name, address), are necessary to give their clients a good and fast service.

2. EMPLOYER/EMPLOYEE RELATIONSHIP

In particular, it should be possible to give consent in the employment relationship. The presumption that the employment relationship is of questionable nature in preamble 34 concerning consent is unfounded and unacceptable. In the employment context consent is often given in areas where it is in the employees' interest that their personal data is processed. Otherwise, employees would be deprived from deciding how their personal data is used. For example it is beneficial for the employers and the employee that the employee in relevant situations can consent that the employer process information with regard to his/hers health, holiday, parental leave, income tax, criminal convictions, education, and wage.

Example 1: In Belgium the consent of the employee is, amongst others, used as the legal basis for transferring specific data of employees from an affiliate or subsidiary company to the mother company located outside of Europe. This is allowed on the basis of article 22, §1, 1° of the Belgian privacy act (cfr. Art. 44 of the proposal). This kind of operation is not harmful for the employees. In many cases it's even an advantage for them, because it leads to more employee mobility within multinational companies.

Example 2: Another example can be found in the area of the private employment agencies and recruitment offices. When a candidate employee presents himself at such an agency/office in Belgium, it is crucial that the agency/office transmits some of his personal data (e.g. his curriculum vitae) to candidate employers. The personal data are thus processed in order to help the candidate employee find a job. The candidate employee is asked to give his consent for this.

Example 3: In Germany, the consent is, amongst others, used as the legal basis to publish contact details and photos of their employees on the company website. This allows clients to directly contact the responsible person in charge. Without the possibility of the employee to give consent on the publication of his or her photo the employer is not able to maintain this important service for the customer-client relation in the future.

3. CONSENT IN PROCESSING PERSONAL DATA OF A CHILD

Regarding consent in the context of processing personal data of a child, the proposal lacks clarity concerning the harm to children it aims to prevent. It seems that mere processing of personal data of children is seen as harmful. However, one should identify types of processing that are harmful and focus on preventing those.

Article 8 needs further clarifications regarding when information society services are "directly offered to a child" and what ""verifiable consent" of a child's parent or custodian is. To avoid hampering the development of services addressed to children,

such as educational ones, the article should also explicitly clarify that consent might be obtained by electronic means.

The proposed definition of 'child' in article 4 may also pose problems between different Member States where currently national legislation defines this differently based on national preferences and stemming from different historical origins.

MINIMUM PROCESSING PRINCIPLE (ARTICLE 5)

The Commission proposal stipulates that personal data must be limited to the minimum necessary in relation to the purposes for which they are processed. While data minimization is an important principle that tries to assure proportionate and relevant collection of information regarding its use, such a provision might lead to a situation in which a supervisory body will question the scope of data collected, even if the data subject gave its consent for the processing. The regulation should not replace the ability of the individual to control the use of their information and should focus more on the rules related to data processing as opposed to the material scope of collected and processed data where it has been consented to.

LAWFULNESS OF DATA PROCESSING (ARTICLE 6)

This article sets out the criteria within which it would be lawful to process personal data, and is therefore a very critical part of the proposed regulations. It is therefore also very important that this article is proportionate and avoids unintended consequences.

Firstly, the article should clarify under 6(c) that processing is necessary where the data controller needs to comply with domestic or international regulations (such as financial regulations) guidance and industry codes of practice as well as legal obligations. Furthermore, article 6 paragraph 1 (b) and (c) of the draft regulation provides that processing of personal data must be possible in performance of a contract or a legal obligation. This fails to take adequate account of national specificities.

For instance, in Germany and other Member States collective agreements such as sectoral and company-level agreements rank equally with legislation enacted by the state and hence can provide the basis for legal data processing. Collective agreements guarantee a balanced level of data protection. In this regard, the company-level agreement serves primarily to give concrete form to unspecified legal concepts in data protection legislation for companies and their employees and to organise legally secure procedures. For this reason, such rules meet the objective of practical data protection in a better and more sustainable way than statutory requirements. Hence, it must be ensured that collective agreements such as sectoral and company-level agreements can remain a legal basis for data processing.

Example of company-level agreements: Introduction and use of an employee identification card (including the possibility for cashless paying in the staff restaurant), implementation and analysis of employee surveys.

Secondly, it is essential that data processing for the legitimate interests of third parties under 6 (f) must continue to remain possible as under the 1995 data protection directive, provided that the necessary conditions are met. This is indispensable for the day-to-day business activities of many companies such as in magazine publishing, where the use of third party addresses is important for reaching new customers. Without the modification of this paragraph contacting customers would be limited to only current readers.

RIGHTS IN RELATION TO RECIPIENTS (ARTICLE13)

An obligation on controllers to communicate any rectification or erasure to each recipient would be very burdensome. It would always involve "disproportionate effort", especially with regard to technical or unessential rectifications. Also in cases when data are disseminated for example on an internet website or in places open to the public, exercising recipients' rights could lead to a situation in which, following a data subject's request to erase personal data, the data would have to be made public again.

RIGHT OF ACCESS FOR DATA SUBJECT (ARTICLE 15)

It is appropriate that data subjects should have access to their personal data.

However, the proposal to waive the fee for processing subject access requests risks leading to a significant increase in frivolous requests, which would be difficult and expensive for companies to manage. A nominal fee as in the current directive helps weed out such requests resulting in a more proportionate and manageable for businesses to process system. Alternatively, a time restriction for such requests could be considered as is the case in the Polish law on data protection, according to which a request can be submitted once every 6 months.

RIGHT TO BE FORGOTTEN AND TO ERASURE (ARTICLE 17)

It has to be underlined that this new right will have negative consequences for the transaction models of online services and for the functioning of banks, credit registers and other institutions, which for the purpose of safeguarding further transactions and detect potential abuses to prevent fraud, process personal data related to credit or transactional history.

Example 1: Allowing a person with bad credit history to demand for its erasure might hamper responsible lending and have serious economic consequences. Erasure of credit history can be also disadvantageous for a person who fulfilled his/her credit obligations in the past and would like to obtain another credit.

Example 2: Buying platform where comments of users on a seller/buyer performance are the main source of verifying somebody's credibility. If an unfair seller is allowed to ask for erasure of all of his data after closing his account on the platform, how can a data controller assure that the same user will not open another account and continue fraudulent transactions?

It should be noted that the intention of this article is to delete data allowing for identification of a natural person from a public perspective (and not with the use of internal structures of the service provider, where such data should still be kept due to security policy and other applicable provisions of law). Moreover, it is required to separate personal data processed by an administrator from personal data published by a data subject (hosting) on which an administrator has no impact as to its publishing.

Furthermore, it should be stressed that the provisions obliging controllers to remove all the links are in many cases practically impossible, since they would require them to determine who had access to disseminated information and who copied it. It is not possible to effectively inform third parties (including those who were not authorised by the controller to publish personal data) about a request made by a data subject, because it is unworkable to determine who copied the data which was made public or which websites refer to these data.

Lastly, one should recall that requirements already exist to retain information for only the amount of time relevant to the use and purpose of collection. This obligation flows with the information so that each party that receives information has such obligations. Under the right to be forgotten such obligation is placed on the initial collector of the information with, as highlighted above, unworkable obligations to delete information on sites beyond their control. It would seem that the proposed solution is both less workable and more limited in coverage than the existing obligations. Ultimately this new right will be confusing for consumers, since there are many situations in which personal data cannot be erased for valid and legal reasons.

DATA PORTABILITY (ARTICLE 18)

The Commission proposal introduces a new right to data portability which is designed to allow individuals to change services more easily by giving them the right to obtain a copy of their data from the controller in an electronic format making it possible to transfer their personal data to another service provider. This proposal also allows the Commission to specify technical standards for the transmission of data, which goes against the principle of 'technological neutrality'.

The proposal does not really reflect the technical reality. Data received from a controller cannot be easily – or at all – used as it is in other services as e.g. companies have different kinds of formats and ways of processing data that are designed to fit with the other aspects of their services and products.

In practice, the proposed right could mean that processor would have to collect the required data from different data bases as companies may have more than one database. After this all data should be transformed into a format that may not be used by the companies for its own purposes. If this process cannot be automated (automation would naturally mean costs as well), it would require human resources.

We fully support the data subjects' right of access and right to object as defined in the current data protection regime but cannot support the proposed right to data portability. This proposal does not belong to a data protection legislation piece.

RIGHT TO OBJECT (ARTICLE 19)

The proposal transfers the burden of proof from data subjects, who under the current directive have to show their particular situation to controllers. According to the proposal, the later would be obliged to demonstrate "compelling legitimate grounds for the processing" even if they process the data in accordance with article 6. This solution will impose another burden on administrators and needs to be revised.

PROFILING (ARTICLE 20)

A balanced regulation of profiling is important for ensuring consumer trust.

However, the proposed changes in the Commission proposal in relation to measures based on profiling lack clarity. If the proposal is meant to cover many rather routine data processing operations that are developed to satisfy consumer demand (e.g. services that remember consumers' preferences), it fails to acknowledge the fact that profiling is often a basis for a good customer service and not always simply a means for additional marketing. Additionally, in certain sectors profiling is a necessity (for instance in the insurance or banking sectors).

Provisions on profiling need to allow profiling for legitimate interests and purposes that are for e.g. intended to respond to consumer demands. In other words, there is no need to require additional and specific conditions for this type of profiling.

RESPONSIBILITY OF THE CONTROLLER (ARTICLE 22.3)

This provision adds layers of burdensome bureaucracy for businesses and supervisory authorities, at they are obliged to assess the adequacy of the measures adopted in order to fulfil the general obligations and be legally responsible in case of breaches. On the other hand, the scheme of responsibility proposed by the regulation considers data processing as risky, and therefore giving the controller the burden of proof. Accordingly, it is the controller who is obliged to demonstrate that it has adopted all the necessary measures to avoid the damage and that the damage was not ascribable to it.

As a consequence, recruiting "independent internal or external auditors" to verify the effectiveness of the measures should be subject to the free choice of the controller. Assuming this, paragraph 3 of article 22 should be deleted and the following paragraph 4 should be modified adapting the references to the verifications of effectiveness.

DATA PROTECTION BY DESIGN AND BY DEFAULT (ARTICLE 23)

The proposed regulation contains new provisions on data protection by design and by default.

While we consider both valuable guiding principles for companies, they should not be dictated in a top-down way in a regulation, which ignores the specific context of the circumstances of the company, the nature of the information, the infrastructure and

numerous other factors. The provision on data protection by default is an example of a poorly defined rule that will create legal uncertainty. Instead it should aim to set clear expectations for what privacy by default should achieve while allowing flexibility for how each company should set about achieving it.

Industry is best placed to determine what constitutes privacy by design applied in practice and we strongly question the need for articles 23.3 and 23.4 legitimizing the European Commission's power to propose delegated acts and technical standards via implementing acts."

PROCESSOR AND CONTROLLER RELATION (ARTICLES 4, 24 AND 26)

The proposed regulation specifies in article 4.6 the definition of the processor, as processing "on behalf of the controller" and, as mentioned in article 26, "only on instructions from the controller". It is also stipulated in article 26 that the carrying out of processing between processor and controller is governed "by a contract or other legally binding act".

In case of erroneous process, the articulation between articles 26.4 and 24 is unambiguous: If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in article 24.

For example, the proposed regulation requires the processor to provide full documentation on the data processing (Article 28). In reality, most processors do not have the knowledge required to fulfil this obligation (for example, a cloud computing provider). The processor would be fully liable for the data processing carried out by it on behalf of the controller (Article 77). The processor might not even know the content of the processing carried out. In addition, it would become much more difficult to engage data processors, because the controller has to specify the conditions of the data processing (Article 4 (5)), which takes away flexibility needed to provide cost efficient services and adds substantial bureaucracy.

We see incoherence and inconsistency in several provisions of the draft regulation, leading to confusion between the controller and the processor obligation. It imposes for instance several obligations without distinction between processors and controllers (designation of a Data Protection Officer (DPO) – article 35; documentation requirements – article 28 etc.).

Under the current directive, processors are directed by controllers on what to do with the data they are provided. They rely on the controllers' assertions and instructions related to the data and act accordingly pursuant to the terms of the contractual arrangement between them. With the new proposals, processors will no longer be able to rely on controller assertions related to the data. They will need to have independent knowledge of the data needlessly expanding the scope of persons with detailed knowledge of the data. Furthermore processors will no longer be able to rely on controllers' instructions related to the data as they will need to evaluate those instructions in relation to their obligations. Since there is more than one compliant way to treat the data, this will decrease legal certainty and undermine the trust in the

controller processor relations. Processor obligations should continue to be controlled by and specified in contractual clauses between controller and processor.

A clear distinction should be made between the liabilities of the controller and those of the processor. In practice it would become confusing if both parties are liable for the same obligations.

Since the controller decides for which purposes the processing of personal data is done, he should be sole responsible for this. In his contract with the processor he should foresee the necessary guarantees to allow him to recover the damages that are due to the processor.

Example 1: The notification of a data breach to the national authority should be an obligation for the controller, not for the processor. The controller should however foresee in his contract with the processor that the processor should notify him of any data breach. (article 31)

Example 2: Only the controller should be liable for the mandatory privacy impact assessment. (article 33 and recital 66)

Other examples of this unnecessary double liability can be found in the articles 28 (documentation), 29 (co-operation with the supervising authority), 30 (security of processing), 34 (prior authorization and prior consultation), 35 (DPO) and 77 (right to compensation and liability).

For the same reasons as those mentioned above, the requirement to ask the prior permission of the controller before enlisting another processor (sub-contractor) is not acceptable (Article 26.2 (d)).

DOCUMENTATION, PRIVACY IMPACT ASSESSMENTS AND PRIOR CONSULTATIONS AND AUTHORISATIONS (ARTICLES 28, 33 AND 34)

1. DOCUMENTATION

The proposal introduces far-reaching documentation obligations as well as requirements on data protection impact assessments and prior consultations and authorisations which would significantly increase administrative burden for both controllers and processors.

The proposed documentation obligations are very detailed and the Commission is mandated to lay down standard forms for the documentation. We believe that data processing can be documented well in many ways and no specific method should be mandated. The obligation is disproportionate since it covers almost all processes. Documenting will be a very extensive process. The obligation will trigger high costs also for low-risk processes.

Example: The Italian privacy code (article 37), in line with articles 18 and 19 of the Directive 95/46/CE, limits the obligation of notification only to some kinds of data processing, namely to the risky ones, while the new obligation proposed would be to maintain all the documentation with no distinction. Moreover, this obligation does not indicate a maximum period for the maintenance of the documentation. This way, the new provision would introduce an unjustified burden for controllers, who would have no option but to fill hundreds of documents a day (for enterprises) including information already made known before.

As a consequence, Article 28 should be deleted as well as all references to it within the regulation (e.g. Article 22 paragraph 2a).

2. PRIVACY IMPACT ASSESSMENTS/PRIOR CONSULTATIONS

While the general obligations of diligence and planning should be maintained, prescriptive provisions on privacy impact assessments risk creating a 'tick-box' approach to data protection and should be re-considered. Privacy impact assessments are internal processes designed to identify and remedy risks to systems and processes in their development. Trying to turn such processes that often contain sensitive and proprietary organisational information into public accountability processes undermines the very essence of the process. There is no question that the results of such assessments may provide useful information to Data Protection Authorities in specific investigations or review of corporate processes. However, there should not be an obligation to file them in the ordinary course or otherwise publish results. We cannot emphasise strongly enough, how important a flexible framework is.

The proposed provisions on privacy impact assessments and prior consultations will add layers of burdensome bureaucracy for businesses and supervisory authorities but also consumers without reflecting best practices of planning and assessment work done by companies. One should also recall that simple registration filings were faced with substantial, sometimes multi-year, backlogs at many of the Data Protection Authorities. Delays in processing assessment of systems could severely impact the speed of deployment and implementation of systems limiting both innovation and competitiveness in the EU. There should be no prior consultation obligation for data processing which according to the assessment is in compliance with data protection legislation.

Also the obligation to consult data subjects or their representatives should be deleted or limited to specialised categories of data where the risks are high as it could e.g. risk the confidentiality of information and trade secrets, if a blanket approach is adopted.

Example 1: Article 33 foresees a mandatory privacy impact assessment where processing operations represent specific risks. The cost of such a privacy impact assessment is estimated between € 10.000 and 30.000, which is disproportionate.

Example 2: This obligation risks re-introducing in the Italian legal system a merely formal and bureaucratic document (so called “DPS”), with no utility with regard to data protection as it is only a collection of information and a description of overall aspects of data processing. The experience reached within the Italian system proves that such a fulfilment brings only useless costs and burdens, with no benefits in terms of data protection.

DATA BREACH NOTIFICATIONS (ARTICLES 4, 31 AND 32)

Mandatory notification requirements for all breaches, even minor ones, would impose significant compliance burden not only on controllers but also on supervisory authorities. They would aggravate “notification fatigue” amongst consumers and give them a false picture of security regarding companies. Only companies with good security will be able to identify breaches. Providers with poor security will fail to identify and notify any breaches. Therefore, they will appear secure for the end-users.

It should also be stressed that the 24-hours deadline for data breach notifications is in many cases unrealistic. Very often internal verification procedures of companies, aiming at assessing whether a data breach took place, last longer than 24 hours. If data breaches are notified before verification has been completed, this will lead in a series of corrective notifications and these will not improve data subjects’ trust.

Instead of the current proposal, a duty to notify the supervisory authority and data subjects without undue delay (but without strict deadlines) could be justified in data breaches that cause serious harm to data subjects and require action by data subjects to minimize the harm. Even in that case, the definition of data breach should be narrowed since the scope is too wide to be workable.

In addition, the obligation offers insufficient incentives for applying effective privacy-measures. Even when encrypted -non readable- data are lost, the supervisory authority should be notified. This is disproportional and does not stimulate organizations to take certain measures. An exception for encrypted 'data' should be in place.

Example: A company manager loses his or her laptop, containing personal data of another data subject. This laptop however is very well secured (encoded, encrypted) and so it is highly unlikely that the person who finds/stole it will be able to access the information on the laptop. In cases like these a notification to the supervisory authority has no added value.

DATA PROTECTION OFFICERS (DPOS) (ARTICLES 35, 36 AND 37)

The proposed regulation would make data protection officers mandatory for all public authorities, companies employing more than 250 persons, or controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects.

The proposal grants DPOs with a strong position (at least a two-year appointment, vague basis for dismissal). In addition, management should have the right to manage and dismiss the DPO according to collective agreements on the labour market.

Different kinds of organizational set-ups can result in effective data protection and current practices in Member States should be respected. Prescriptive and detailed provisions would be costly and burdensome in particular for organisations where data processing forms only a marginal part of their activities.

If such a regulation is adopted, companies with a DPO should be released from bureaucratic data reporting obligations in return.

TRANSFERS BY WAY OF APPROPRIATE SAFEGUARDS (ARTICLE 42)

Companies often have to transfer data to a third country or international organisation and this article provides safeguards for those transfers. The increased requirement for consent for international transfers risks disrupting emerging digital business models. For example in the newspaper industry, this will be feasible where consumers pay for content and already have a contract with the consumer, but will be much more difficult for free access models, where this requirement could impose a new relationship between the newspaper and the reader.

The requirement to obtain authorisation from the supervisory authority where transfers take place on the data controller's own standard contract clauses (Article 42(2)(d) contract clauses between the controller or processor) is also bureaucratic and burdensome and likely to lead to unnecessary delays in doing business.

The proposed regulation should specifically include the EU-U.S. Safe Harbor program as an appropriate safeguard enabling data transfers. Although as we understand from various communications that the Safe Harbor remains in place under the proposed regulation, it will be important to refer explicitly to this mechanism in an article or recital in order to avoid confusion.

BINDING CORPORATE RULES (ARTICLE 43)

Even though Binding Corporate Rules (BCRs) are more streamlined than in the past and work effectively once established, the administrative burden they continue to pose should be addressed. The utility of BCRs can also be enhanced by expanding their applicability across not just within groups of companies. If a company and its subsidiaries have a valid BCR it should be possible for them to transfer data to another company with a valid BCR. Today global information flows are not limited within groups of companies but exist across value chains. The regulation should reflect and enable that reality.

In order to reduce bureaucratic burden, intra-group data transfers have to be simplified. Unfortunately, the European Commission has not taken the opportunity to create a provision on intra-group data transfer which ensures legal certainty for data transfer not only within the EU but also beyond. The new data protection provisions envisaged with the regulation must be used to close this gap.

BUSINESSEUROPE

POSITION PAPER

COMPETENCE OF SUPERVISORY AUTHORITIES (ARTICLE 4, 51)

BUSINESSEUROPE supports the "one-stop shop" approach enshrined in the draft regulation as it should simplify relations between businesses and supervisory authorities.

However, the regulation has to make sure that the single competent authority is comprehensively informed about all aspects which are relevant in the case concerned. The current wording of the proposal raises the need of clarity in the definition of main establishment (« *where the purposes, conditions and means of the processing of personal data are taken* ») and in the criteria to solve conflicts regarding the role of the supervisory authorities in cases of a business carrying out its activities in several Member States.

ADMINISTRATIVE SANCTIONS (ARTICLE 79)

The proposed regulation introduces very high administrative sanctions for violations based on a "one-size-fits-all" approach.

Example 1: Article 79.5.b. states that the supervisory authority *shall* impose a fine up to € 500.000 or 1% of an enterprise's worldwide turnover, to anyone who, *intentionally or negligently*, does not comply with the right to be forgotten or to erasure.

Example 2: Article 79.6 (h) foresees a fine of € 1.000.000 or 2% of an enterprise's worldwide turnover in case they intentionally or negligently, do not alert or notify a personal data breach.

BUSINESSEUROPE considers a competition law approach regarding the system of sanctions as inappropriate and unacceptable in the context of data protection legislation. In competition law, the sanction system is based on economic studies and understanding of the negative impacts of anti-competitive behaviour to the market dynamics which justifies the turnover-based way of calculating fines. This is not the case for the proposed administrative sanctions.

Even though effective and high- quality enforcement is essential, the proposed sanctions are excessive and disproportionate. Any sanction levied should be proportionate to the impact on data subjects. In our view, particularly in cases of first and non-intentional non-compliance, a warning procedure as well as pre-requisites for renouncing from inflicting sanctions should be considered (for ex. in case where a controller removed the risk of data protection breach and took all measures to avoid them in the future.).

Finally, there is no question that the application of the new regulation will lead to confusion. It will be difficult to differentiate between good faith efforts at compliance and mere negligence in the early stages of its application. Clearly greater emphasis should be placed on intentional violations of the regulation.

BUSINESSEUROPE a.i.s.b.l

AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

Reconsideration on the nature grouping and scope of transgressions in relation to fines should also occur as many minor and administrative failures of compliance are associated with a disproportionate range of fines. There should be a mechanism that gives companies the possibility to defend themselves against the allegations made by the supervisory authority (e.g. a right to be heard before any decision is taken). Supervisory authorities should not be obliged to fine shortcomings.This draconian and disproportionate range of fines may also have a chilling effect on digital innovation in the EU at a time when it can ill afford such potential limitation on growth and economic development.

COLLECTIVE REDRESS (ARTICLE 73, 75, 76)

Although support to data subjects regarding data protection is useful, the taking over by bodies, organizations or associations and bundling of supposed infringements will lead to business models based upon buying and exploiting claims. This will create a claim culture, where organizations will stop innovating or will have to take insurance policies, at the expense of the consumer cost or products and services. In addition, the European Commission is still assessing an overall approach to collective redress in the EU. Therefore, we believe it is inappropriate to come forward with a sector-specific proposal, before a general framework is agreed.

DELEGATED ACTS AND IMPLEMENTING ACTS (ARTICLE 86)

The proposed regulation includes 26 provisions that grant the Commission the power to adopt delegated acts and 19 provisions that allow the Commission to adopt implementing acts. There is hardly an issue that would not be substantially affected by delegated or implementing act. This is in many instances contrary to article 290 of the TFEU, which limits the use of delegated acts to “other than essential elements of an area”.

The numerous provisions on secondary rulemaking undermine legal predictability and risk neutralising the effectiveness of the provisions by complicating the data protection regime. They would mean that legislation would be constantly evolving and achieving compliance would be extremely difficult. The problematic nature of the provisions is further underlined by the fact that compliance with data protection legislation often requires significant and time-consuming data system investments.

We therefore call for a review of the provisions on secondary rulemaking and a limitation of the provisions on delegated acts and implementing acts, when justified, only to non-essential elements. Delegated acts and implementing acts should not for e.g. mandate business processes or technologies.

PROCESSING OF PERSONAL DATA AND FREEDOM OF EXPRESSION (ARTICLE 80)

The current directive allows companies in the business of journalism appropriate allowances to process personal data in the interests of freedom of expression.

In the context of the proposed regulation, it would be helpful to have more certainty around the freedom of expression exemption (Art 80) as this could be of concern for news businesses (i.e. to avoid that Member States decide what the freedom of expression exemption should look like). Unless there is more clarity in the proposed regulation we could have a situation where information from a news story had to be deleted in one jurisdiction but not in another due to countries applying different balancing tests.

RELATIONSHIP BETWEEN REGULATION AND DIRECTIVE 2002/58/EC (DPEC)

Many businesses will be subject to obligations under both the Regulation and DPEC. The wording of Article 89 paragraph 1 is not straightforward to apply, although it appears to be on the face of it.

We need further clarity to understand how the delineation between the two is intended to operate in practice.

* * *